Yui Kee Computing Ltd.

Newsletter

August 2005

Contents

Incident Update

- Wed Aug 3 13:16:42 2005 CA: Win32.Mydoom.O Medium
- Mon Aug 8 16:32:16 2005 CA: Win32.Mytob Family Medium
- Fri Aug 12 17:31:46 2005 FSC: Several new Bagles spreading 2
- Sun Aug 14 20:01:50 2005 FSC: Zotob worm exploiting MS05-39 2
- Mon Aug 15 17:46:36 2005 CA: Win32.Lovgate.AB Medium
- Wed Aug 17 07:01:27 2005 NAI: W32/IRCbot.worm!MS05-039 High
- Wed Aug 17 07:31:37 2005 SARC: W32.Esbot.A L3
- Wed Aug 17 08:01:52 2005 SARC: W32.Zotob.E L3
- Wed Aug 17 08:31:34 2005 TREND: WORM_ZOTOB.D Medium
- Wed Aug 17 08:46:40 2005 TREND: WORM_RBOT.CBQ Medium
- Wed Aug 17 10:01:20 2005 CA: Win32.Peabot.A Medium
- Wed Aug 17 12:16:35 2005 CA: Win32.Tpbot.A Medium
- Mon Aug 29 12:16:40 2005 CA: Win32.Lovgate.AB Medium
- Wed Aug 31 04:46:53 2005 TREND: WORM_ZOTOB.E Medium

Editors Notes

There are several items of note this month. The publication of the first MSH viruses is only of passing interest: there is a new programming environment so there is the possibility of viruses targeting that environment, the news that it has been done only confirms the expected.

The small outbreak of a mobile virus at a major sports event is of more interest. Viruses on mobile phones and other such devices have been a possibility for years, but the outbreak shows the number of such devices is reaching the “critical mass” where epidemics can occur. We can

expect more outbreaks, and more serious outbreaks in future. If your organisation relies on mobile communications contact us to discuss protection strategies.

The exploit of MS05-039 and the associated outbreaks is further evidence that the "time to exploit" was a myth. Could the bad guys have reverse-engineered the patch, developed an exploit and packaged it in a worm or backdoor in just a couple of days, or were at least some of them already aware of and using the exploit (in a low-profile manner, so as not to be noticed), and therefore ready to release a mass attack when the patch was published? Whatever the case, as defenders our assumption should be that the attackers already know all the vulnerabilities, and we must rely on defence in depth to make things difficult for them.

First MSH Viruses

An Australian virus writer has published five viruses that target the Microsoft Command Shell (MSH). MSH is a replacement for shells including CMD.EXE, COMMAND.COM and 4NT.EXE, it was rumoured to included in Microsoft's upcoming Vista operating system, though Microsoft has now confirmed it will not be included.

The virus family as been named Danom and, as "proof-of-concept" viruses, they are unlikely to spread in the wild. Especially as the environment they target has not been released yet.

Eric Chien of Symantec predicted the possibility of MSH viruses in his Virus Bulletin Conference paper last year.

More information:

http://www.f-secure.com/weblog/archives/archive-082005.html#00000613

http://www.f-secure.com/v-descs/danom.shtml

http://www.f-secure.com/weblog/archives/archive-082005.html#00000615

http://www.theregister.com/2005/08/04/vista_virus/

http://it.rising.com.cn/newSite/Channels/Anti_Virus/Virus_Alert/Virus_New/200508/08-100520214.htm

Mobile Virus Outbreak

The Cabir mobile phone virus was reported to be spreading at the Athletics World Championships, held in Helsinki this month. Cabir infects phones running the Symbian Series 60 operating system, and spreads via Bluetooth connections. Apart from draining the batteries of the infected phones, Cabir does no damage.

Users need to accept a download for the phone to be infected, and security researchers speculated that people did so simply to stop the annoyance of repeated permission requests. A safer reaction would be to shut down Bluetooth, or move out of range of the infected device.

More information:

http://www.f-secure.com/weblog/archives/archive-082005.html#00000621

http://www.theregister.com/2005/08/12/cabir_stadium_outbreak/

Malware Outbreaks Targeting Recent Microsoft Vulnerability

Among the three Critical patches released by Microsoft on Tuesday 9th August was one to fix a vulnerability in Plug and Play, MS05-039. The vulnerability has since been exploited in a number of new worms and backdoors, including the Zotob family, Backdoor.Win32.IRCBot.es, Backdoor.Win32.IRCBot.et and W32/Dogbot-A. F-Secure has graphed the relationships between the worms.

Reports have included large organizations with a master firewall, but no internal controls and unpatched machines. Once one machine was infected (possibly a laptop that was infected elsewhere and then connected to the internal network), all vulnerable machines on the network quickly became infected.

Victims have included major news organization CNN, ABC and the New York Times. Microsoft was reported to be in "emergency response" mode, Debbie Fry Wilson, director of Microsoft's security response center, said, "Right now, we're mobilizing our two war rooms".

Researchers at the Internet Storm Center recommended three best practices to mitigate the vulnerability:

- close port 445 at least at the perimeter.
- patch systems quickly.
- eliminate NULL sessions.

Mikko Hypponen of F-Secure has written a personal account of the outbreak.

More information:

http://www.f-secure.com/weblog/archives/archive-082005.html#00000618

http://www.f-secure.com/weblog/archives/archive-082005.html#00000626

http://www.f-secure.com/weblog/archives/archive-082005.html#00000631

http://www.f-secure.com/weblog/archives/archive-082005.html#00000635

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

http://www.f-secure.com/v-descs/zotob_a.shtml

http://www.f-secure.com/v-descs/zotob_b.shtml

http://www.f-secure.com/v-descs/zotob_c.shtml

http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=42446

http://vil.nai.com/vil/content/v_135491.htm

http://www.sophos.com/virusinfo/articles/microsoft0805.html

http://www.sophos.com/virusinfo/articles/zotob.html

http://www.sophos.com/virusinfo/articles/moreworms.html

http://www.sophos.com/virusinfo/articles/breakingnews.html

http://www.f-secure.com/v-descs/ircbot_es.shtml

http://www.f-secure.com/v-descs/ircbot_et.shtml

http://www.sarc.com/avcenter/venc/data/w32.esbot.a.html

http://www.sophos.com/virusinfo/analyses/w32dogbota.html

http://www.sophos.com/virusinfo/analyses/w32tpbota.html

http://www.cnn.com/2005/TECH/internet/08/16/computer.worm/index.html

http://isc.sans.org/diary.php?date=2005-08-16

GIMP reveals PINs

University of Cambridge researchers used the open-source image manipulation software GIMP to reveal the hidden text on supposedly "tamper-proof stationery". However, any

similarly-featured graphics package, commercial or non-commercial, could be used in the same way.

Banks and other organizations that rely on such stationery to deliver PINs and other confidential information should consider alternatives to keep their customers safe.

More information:

http://www.theregister.com/2005/08/25/pin_number_security/

German Association for Technical Inspection certifies Sophos Anti-Virus

The German Association for Technical Inspection (TÜV) has confirmed the effectiveness of Sophos's anti-virus solutions in a series of extensive tests for the second year running. Sophos Anti-Virus was tested on Windows 2000 Professional SP4 and on Windows XP Professional SP2. The Sophos scan engine proved itself on all platforms with excellent results and a 100% virus detection rate.

TÜV Saarland awarded the certificate after conducting a series of comprehensive tests. The test of Sophos Anti-Virus was based on the in-the-wild virus collection of The WildList Organization, containing 1,210 different viruses and worms.

Sophos Anti-Virus identified all malicious files without fault and notified the testers as soon as they tried to access, open, execute or copy infected files. The product was also tested for false alarms - correctly making no mistakes when scanning virus-free data.

"Malicious viruses and worms are sadly part of the networked world, and increasingly widespread. Sophos is continually working professionally and responsively to protect businesses effectively from electronic malware," said Pino von Kienlin, managing director of Sophos GmbH. "The test results of TÜV prove once again, that our customers can rely on all our solutions."

Last year, Sophos was the very first vendor of IT security software to receive the prestigious certificate.

"Good Worms" are a Bad Idea

This is not the first time this has been said, but Paul Ducklin is characteristically entertaining on the topic in the wake of the Zotob worm outbreaks:

http://www.sophos.com/virusinfo/articles/goodvirusbadidea.html

The Devil's InfoSec Dictionary

Confused by information security technical terms? Check the Devil's InfoSec Dictionary.

http://www.csoonline.com/read/080105/debrief.html

Two Zotob Arrests

Cooperating with the US-based FBI, Moroccan authorities have arrested Farid Essebar (alias "Diabl0") aged 18 and Turkish authorities have arrested Atilla Ekici (alias "Coder") aged 21. The suspects allegedly used the information stolen from infected computers for bankcard forgery.

Graham Cluely of Sophos praised the speed of investigation, "Astonishingly the time between virus outbreak and arrest is less than two weeks. The authorities were able to investigate

quickly and co-ordinate internationally to affect arrests in Morocco and Turkey." Experts at Sophos and F-Secure have linked the “Diabl0” nickname to many other viruses.

The FBI and Turkish Authorities have since identified 16 more suspects, although they have not yet been arrested.

Microsoft provided technical expertise in tracing and identifying the suspects. Brad Smith of Microsoft explained, "From the worm's real-time attack, (the investigators) could derive technical information about what was going on." This is a in contrast to the Sasser case, where Sven Jaschan was turned in by “friends” for a reward.

More information:

http://www.map.ma/eng/sections/general/young_moroccan_hacke4792/view

http://www.f-secure.com/weblog/archives/archive-082005.html#00000639

http://blogs.washingtonpost.com/securityfix/2005/08/arrest_of_zotob.html

http://www.sophos.com/virusinfo/articles/wormarrests.html

http://www.f-secure.com/weblog/archives/archive-082005.html#00000641

http://www.sophos.com/virusinfo/articles/diablo.html

http://www.sophos.com/virusinfo/articles/botgang.html

http://www.theregister.com/2005/08/30/zotob_suspects_arrested/

http://www.theregister.com/2005/08/30/zotob_arrests_follow-up/

The End of the Internet?

Scott Grannerman of Security Focus discusses the blanket blocking of Chinese IP addresses by some system administrators. Similar blanket blocks have also been seen in relation to spam. If system administrators block innocent clients at a whim, do we still have an Internet?

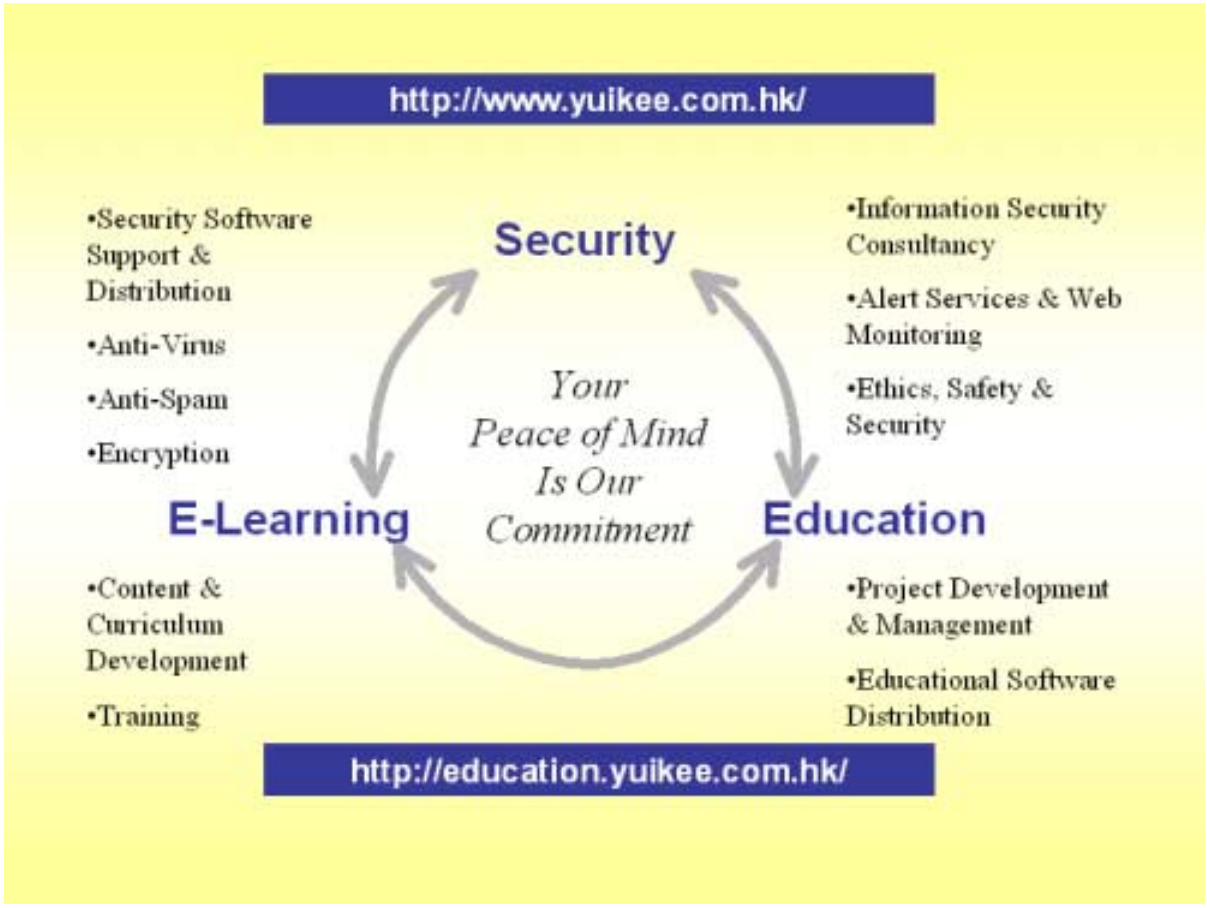
Conspiracy theorists may like to consider how a regime might improve the effectiveness of its censorship by similar means.

More Information:

http://www.theregister.com/2005/08/31/blocking_chinese_ip_addresses/

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/